2006 VIGRE REU Paper

Matthew Bruce

September 13, 2006

1 The Fundamental Theorem of Algebra - Proof 1 (Topological)

Definition 1. *Winding Number*

The winding number of a curve, λ with respect to a point z_0 is the number of times λ goes around z_0 in a counter clockwise direction.

Property 1. *The Fellow Traveler Property*

Suppose that two functions, $f(x)$, and $g(x)$, are such that $|f(x) - g(x)| < \epsilon$ for some ϵ and $\forall x$ on some circle of radius r, C_r, with $\epsilon < r$. Then $f(C_r)$ and $g(C_r)$ have the same winding number.

Theorem 1. *The Fundamental Theorem of Algebra*

Proof. Suppose that $f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_0$. We can assume without loss of generality that $a_n = 1$. Furthermore, we can assume that $a_0 \neq 0$ otherwise $z = 0$ would be a root. Now, $f(z)$ is a continuous complex polynomial, mapping $\mathbb{C} \Rightarrow \mathbb{C}$. We also know that

$$\lim_{z \to \infty} \frac{z^n}{f(z)} = 1$$

and so for a circle with sufficiently large radius r (C_r), we have

$$|z^n - f(z)| \leq \alpha r^n$$

with $0 < \alpha < 1$ and z on the circle, C_r.

For any $r > 0$, z^n winds C_r around the origin n times. Therefore, by the fellow traveler property $f(z)$ will also wind a sufficiently large C_r, n times around the origin. For a sufficiently small radius r around the origin, $f(z)$ is approximately equal to a_0 and will not wind around the origin at all. Since $f(z)$ is continuous, $f(C_r)$ will depend on r continuously. Since $f(C_r)$ has winding number of 0 for sufficiently small r, and winding number of n for sufficiently large r, it follows that there exists a radius, say r_1, such that $f(C_{r_1})$ passes through the origin. Thus, $\exists z_1$ on C_{r_1} such that $f(z_1) = 0$. This proves the theorem. □

2 The Fundamental Theorem of Algebra - Proof 2 (Analytic)

Lemma 1. *The absolute value of a continuous complex funcion has a minimum value. Let $f(x) \in \mathbb{C}[x]$. Then $|f(x)|$ has a minimum value at some point $x_0 \in \mathbb{C}$.*

Proof. It is clear that $|f(x)| \to \infty$ as $|x| \to \infty$. Thus, for r sufficiently large, the greatest lower bound of $|f(x)|$ on the disk $x \leq r$ is also the greatest lower bound of $|f(x)| \forall x \in \mathbb{C}$. Thus, $|f(x)|$ is a continuous function on a closed and bounded set (compact), and hence attains its minimum value.

□

Lemma 2. *Let $f(x) \in \mathbb{C}[x]$. Then, for any x_0, if $f(x_0) \neq 0$, then $|f(x_0)|$ is not a minimum value of $|f(x)|$.*

Proof. Suppose $f(x)$ is a nonconstant complex polynomial and suppose x_0 is a point such that $f(x_0) \neq 0$. Now make the change of variable $x = x + x_0$. Thus, we may assume that $f(0) \neq 0$. Now multiply $f(x)$ by $f(0)^{-1}$ so that we have $f(0) = 1$. Now, it suffices to show that 1 is not the minimum value of $|f(x)|$. Let k be the largest non-zero power of x. Then $f(x)$ is of the form:

$$f(x) = a_k x^k + \ldots + 1$$

Now let α be the k-th complex root of $-a^{-1}$. Now make the change of variable αx for x and our equation takes the form

$$f(x) = 1 - x^k + x^{k+1} g(x)$$

for some function g(x). Now, using the triangle inequality, for small positive real x we have

$$|f(x)| \leq |1 - x^k| + x^{k+1} |g(x)|.$$

Since x is sufficiently small, we have $x_k < 1$ thus:

$$|f(x) = 1 - x^k + x^{k+1} |g(x)| = 1 - x^k (1 - x|g(x)|).$$

Thus, for small x, $xg(x)$ is small, thus x_0 can be chosen such that $x_0 |g(x_0)| < 1$. Thus $x_0^k (1 - x_0 |g(x_0)|) > 0$, thus $|f(x_0)| < 1 = f(0)$ completing the proof. □

Theorem 2. *The Fundamental Theorem of Algebra If $f(x) \in \mathbb{C}[x]$, and $f(x)$ is not constant, then $f(x)$ has at least one complex root.*

Proof. Suppose $f(x)$ is a nonconstant complex polynomial. Then we know that there is at least one point x_0 where $f(x)$ attains its minimum (lemma 1). We know that $|f(x_0)| = 0$ by lemma 2, thus $f(x_0) = 0$, which completes the proof.

□

3 The Fundamental Theorem of Algebra - Proof 3

Lemma 3. *Any odd-degree polynomial must have a real root.*

Proof. Let $f(x) \in \mathbb{R}[x]$ with degree $f(x) = 2k+1$ for some k. Suppose further (without loss of generality) that the leading coefficient, $a_n > 0$. Then the following limits are true:

$$\lim_{x \to \infty} f(x) = \infty$$

$$\lim_{x \to -\infty} f(x) = -\infty.$$

Thus, there exists some sufficiently large x_0 such that $f(x_0) > 0$, and there exists some sufficiently large x_1 such that $f(-x_1) < 0$. Thus, since $f(x)$ is a polynomial and hence continuous, there exists some x_2 such that $f(x_2) = 0$ by the intermediate value theorem. □

Lemma 4. *Any two-degree complex polynomial must have a complex root.*

Proof. This lemma is a consequence of the quadratic formula. Given $f(x) = ax^2 + bx + c$ the two roots are:

$$x_0 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, x_1 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

We know both of these exist as all complex numbers have square roots. However, if $b^2 = 4ac$ then the two roots will be the same. □

Definition 2. *Splitting Field If $0 \neq f(x) \in F[x]$ and G is an extension field of F, then $f(x)$ splits in G, if $f(x)$ factors into linear factors in $G[x]$. This means that all the roots of $f(x)$ belong to G.*

Lemma 5. *Any nonconstant real polynomial has a complex root.*

Proof. Let $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{R}$ such that $n \geq 1, a_n \neq 0$. Then let us perform induction on the degree n of $f(x)$.

Suppose $n = 2^m a$, where a is odd. Now let us do induction on m. If $m = 0$, then $f(x)$ has odd degree and by the lemma 3 has a root. Now let us assume that the theorem is true for all degrees $d = 2^k b$ where $k < m$ and b is odd. Now assume that the degree of $f(x)$ is $n = 2^m a$.

Let G be the splitting field for $f(x)$ over $\mathbb{R}$ which contains the roots $\alpha_1, \alpha_2, \cdots, \alpha_n$. To prove the theorem we will show that at least one $\alpha \in \mathbb{C}$. Fix an integer $h \in \mathbb{Z}$, and construct the polynomial:

$$H(x) = \prod_{i<j} (x - (\alpha_i + \alpha_j + h\alpha_i\alpha_j)).$$

This polynomial belongs to $G[x]$. The number of pairs of alpha's for any given $n = 2^m a$ is given by

$$\frac{(2^m a)(2m^a - 1)}{2} = 2^{m-1}a(2^m a - 1) = 2^{m-1}b$$

for some odd b. Thus, the degree of $H(x)$ is $2^{m-1}b$.

Now, $H(x)$ is a symmetric polynomial in $\alpha_0, \ldots, \alpha_n$. Since the alphas are roots of a real polynomial ($f(x)$), and $H(x)$ is symmetric in the splitting field, $H(x)$ must be a real polynomial.

Therefore, $H(x) \in \mathbb{R}[x]$ with degree $2^{m-1}b$. By the inductive hypothesis $H(x)$ has a complex root. Thus, there exists a pair of alphas such that

$$\alpha_i + \alpha_j + h\alpha_i\alpha_j \in \mathbb{C}.$$

Now, since h was arbitrary, we can specify some h_1 and get alphas such that:

$$\alpha_i + \alpha_j + h_1\alpha_i\alpha_j \in \mathbb{C}.$$

Since there are only finitely many pairs of alphas, it follows that there must be at least two numbers, h_1, and h_2, such that

$$z_1 = \alpha_i + \alpha_j + h_1\alpha_i\alpha_j \textit{ and } z_2 = \alpha_i + \alpha_j + h_2\alpha_i\alpha_j \in \mathbb{C}.$$

Now, $z_1 - z_2 = (h_1 - h_2)(\alpha_i\alpha_j) \in \mathbb{C}$. Thus, as h_1, h_2 are in $\mathbb{Z}$, we know that $\alpha_i\alpha_j \in \mathbb{C}$. Thus $h_1\alpha_i\alpha_j \in \mathbb{C}$, and further $\alpha_i + \alpha_j \in \mathbb{C}$. Now, let a new polynomial, $p(x)$ be as follows:

$$p(x) = (x - \alpha_i)(x - \alpha_j) = x^2 - (\alpha_i + \alpha_j)x + \alpha_i\alpha_j \in \mathbb{C}[x].$$

Thus, $p(x)$ is a degree-two complex polynomial and thus its roots are complex (previous lemma). Thus, $f(x)$ has a complex root.

□

Lemma 6. *If every nonconstant real polynomial has a complex root, then every nonconstant complex polynomial has a complex root.*

Proof. Let $p(x) \in \mathbb{C}[x]$ be a nonconstant complex polynomial. Now assume that every nonconstant real polynomial has a complex root. Let $h(x) = p(x)\overline{p}(x)$. Now $h(x) \in \mathbb{R}[x]$ and thus has a complex root, x_0. Thus, $p(x_0)\overline{p}(x_0) = 0$, and thus either $p(x_0) = 0$, or $\overline{p}(x_0) = 0$ (as $\mathbb{C}$ does not have zero divisors). Thus, either x_0 is a root of $p(x)$, or $\overline{p}(x_0) = \overline{\overline{p}}(\overline{x_0}) = p(\overline{x_0}) = 0$. Thus $p(\overline{x_0})$ is a root of $p(x)$. □

Theorem 3. *The Fundamental Theorem of Algebra If $f(x) \in \mathbb{C}[x]$, and $f(x)$ is not constant, then $f(x)$ has at least one complex root.*

Proof. Suppose $f(x)$ is a nonconstant complex polynomial. Then by lemmas 5 and 6 since all real polynomials have real roots, and thus all complex polynomials do, $f(x)$ has a complex root. This proves the theorem. □